Your Mission: Use F-Response to access Rackspace CloudFiles



Using F-Response to connect to Rackspace CloudFiles and collect its contents



Disclaimer: F-Response provide access to 3rd party data sources via Application Programming Interfaces (APIs) and internal structures presented by the provider. 3rd party provided data sources by their very nature are volatile. The afore mentioned F-Response products provide "best effort" for accessing and interacting with those 3rd party data sources however service disruptions, API changes, provider errors, network errors, as well as other communications issues may **Important** result in errors or incomplete data access. F-Response always recommends secondary validation of any 3rd party data collection.

Step 1: Open Rackspace CloudFiles Credential Configuration Window

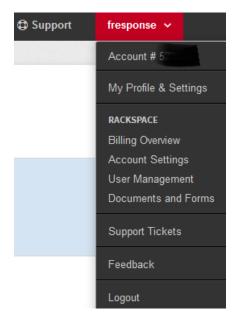
Open the F-Response Management Console and navigate to the Providers->Provider Credentials->Rackspace Cloud Files menu item.

e Providers	Deployment Subj	ects Targets	Image	s Containers	Messages V	iew Help
ovi Prov	der Settings	1	×s	ubjects	×	Targets
Add Drop Goog Goog Imap Micro Micro Offic Offic Offic Offic	der Credentials Offline Email Cache F Dox le Drive For Business le Drive For Consume le Mail (OAuthv2) Email soft Azure Blob Stora soft Sharepoint 2013 e365 Email e365 OneDrive For Bus e365 Sharepoint e Email Cache rive For Consumers pace CloudFiles	rs ge (On Premise)	Box Go Go Im Mii Off Off Off	x.com opbox ogle Drive For ogle Drive For ogle Mail (OA ap Email crosoft Azure I crosoft Sharep fice 365 Email	Consumers uthv2) Blob Storage oint 2013 (On-Pr ive for Business point nsumers	

F-Response Management Console

Step 2: Obtain Rackspace CloudFiles Credentials

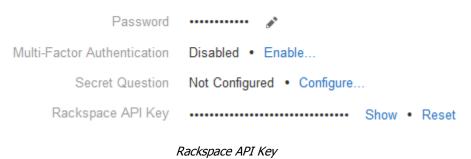
Rackspace CloudFiles Credentials are found on the Rackspace Management Console (see **manage.rackspacecloud.com**). The specific credentials required are available under the "**My Profile and Settings**" menu item for your account, under **Security Settings**, see below:



Rackspace Cloud Management Console Main Page

Locate the Rackspace API Key section, then press "**Show Key**" to view the **API Key** and record (copy/paste) the key.

Security Settings



These credentials (Username and API Key) must be entered in the corresponding fields in the **Configure Rackspace CloudFiles Credentials** dialog in the F-Response Management Console. The **Description** field is not optional and can be used to provide a secondary human readable identifier for the credential set (Ex "Client X Account").

ackspace CloudFiles Credentials ackspace CloudFiles Credentials	
Description	Add
Username	
API Access Key	
	Remove
RackspaceTest	
	ОК

Credentials Dialog

Step 3: Scan and Enumerate Rackspace CloudFiles Targets

Double click on the newly added Rackspace CloudFiles account under the Providers tree. This will scan the provider and result in a listing of available targets in the Targets window.

Providers	× Targets	Targets		
 Providers Amazon Simple Storage Service Box.com Dropbox Google Drive For Business Google Drive For Consumers Google Mail (OAuthv2) Imap Email Microsoft Azure Blob Storage Microsoft Sharepoint 2013 (On Office365 Email Office365 OneDrive For Business 	Pret			
Office365 Sharepoint	Name Local Devic	ce		
Offline Email Cache OneDrive For Consumers Rackspace CloudFiles RackspaceTest				

Listing Targets

Step 4: Login and Mount one or more Rackspace CloudFiles Targets

Double click on an individual target in the Targets window to begin the mounting process. Once attached the share will present a drive letter.

Local Device	Last Status
E:\	

Step 5: Create Image of attached volume

Select the newly attached target and right click on the Local Device column. Use the "Create Image..." option to open the "Image" dialog to begin imaging the device.

Targets				
Name		Local Device Last St		
CaseTestin		EA.		
CASETESTI	Create Imag	e		
Litest4	Open in Win	dows Explorer		
Irs-standard	Open in Cor	nmand Prompt		
rs-jumbo	Open in X-W	ays Forensics		
Irs-empty -				

Start Imaging Process...

Step 6: Complete Imaging Options...

	irtual Device	×
Source Type	 Physical (Includes Unallocated Space) Virtual (Files and Folder Contents Only) 	
Format	E01 ~	
Image Source	(E:\)\\X64-WIN10\CaseTesting ~	
Image Name	RackspaceCloudFiles	
Image Path	M:\	
Hash	Both V Total Available Space = 10193MB	
Compression	None	
Examiner Name	Joe Examiner	
Case Number	#2786	
Evidence Number	0134	
Unique Description	Suspect's Rackspace CloudFiles Account	
Notes	Full image of virtual device, contains Files only.	

We'll work through this window from the top down. First, the **Source Type** is set to **Virtual** (by default) to be able to create an image of the connected virtual device data.

Next you can select the image **Format** you have a choice **E01** (Expert Witness), **VHD** (Virtual Hard Disk), or **Both**. This option determines what the mager will provide at the end of the collection.

Image Source should be populated if we opened this window

from Windows Explorer, just verify the drive letter is correct from Step 1. For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can choose a **Hash** format and the **Compression** level if you wish to compress the resulting image file. The remaining fields are specific to your case and can be filled out accordingly. These fields will be included in the resulting log file for the image.

Once you have all your information entered simply click the **Start Image** button to begin the process.

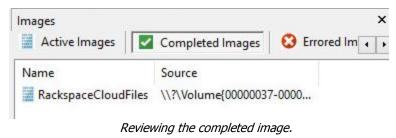
Step 7: Review the Image

Once started the dialog will close and you'll be able to monitor the image using the Active Images. When the Image completes you will see it move to Completed Images.

Active Images	Compl	eted Images	🕄 Errored Im 😱
Name	Source	Last Status	
RackspaceCloud	\\X64	Formatting a	a Volu

Step 8: Review the Completed Image

Right click on the completed image to access the Image Path, Log, and File List. These logs and listing contain details about the image, the image itself, and a file listing of files collected.



Troubleshooting